IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

IN THE MATTER OF THE SEARCH OF)
1. Black and Silver Apple Ipod, Model: A1367, S/N: C3RHX0NGDT75)
2. White and Silver Apple Ipod, Model: A1367, S/N: CCQHWEX1DNQW)
3. Black Motorola Boost Mobile Model: WX430 MEID 268435460405774382)

CASE NUMBER 12-3169-DGW

FILED UNDER SEAL

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

I, David B. Vucich, being duly sworn and deposed state:

I am a Special Federal Officer with the Federal Bureau of Investigation's (FBI) Metro-East Cyber Crime and Analysis Task Force, and I have reason to believe that stored within the following:

1. Black and Silver Apple Ipod, Model: A1367, S/N: C3RHX0NGDT75
2. White and Silver Apple Ipod, Model: A1367, S/N: CCQHWEX1DNQW
3. Black Motorola Boost Mobile Model: WX430 MEID 268435460405774382

which are all within the Southern District of Illinois, and in the possession of your affiant, is now concealing certain electronic data files and digital information of evidentiary value:

SEE ATTACHED LIST, ENTITLED "ATTACHMENT A"

which constitutes evidence of the commission of a criminal offense or the fruits of crime, or which is designed or intended for use or which is or has been used as the means of committing an offense in violation of 18 U.S.C. §§ 2252 and 2252A. The facts to support the issuance of this Search Warrant are as follows:

AFFIDAVIT

I, David B. Vucich, being first duly sworn state:

1. I am a Detective Sgt. with the Madison County Illinois Sheriff's Office. I have been employed by said Department since November 1997. I am currently assigned to the Federal Bureau of Investigation's (FBI) Metro-East Cyber Crime & Analysis Task Force as a Special Federal Officer (SFO), and have been so assigned since approximately 2005. MCCA is comprised of law enforcement personnel from approximately 15 different local, state, and federal agencies. I work with other members of MCCA at the FBI's office in Fairview Heights, Illinois. During this time, I have been trained to investigate and conduct investigations of various types of crime, including computer crimes. The statements contained in this affidavit are either based upon my investigation, information provided by other investigators, other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as a Deputy with the Madison County Sheriff's Office and an SFO with the FBI. As part of my regular duties, I have investigated matters involving the online exploitation of children, particularly regarding the possession, receipt, and transmission of images of child pornography. I have gained expertise in the conduct of such investigations through training seminars, classes, and everyday work related to conducting these types of investigations. I regularly conduct forensic computer and cell phone exams and I have and continue to receive training in the search and recovery of cell phones, computers, peripherals, computer data, imaging computer hard drives, and interpreting on-line computer activity from data logs and Internet Service Providers. I have had involvement, either directly or indirectly, in over 150 online child exploitation investigations and have been the lead case agent in at least 50 of them. I also participate in the execution of federal search warrants.

Introduction

2. This affidavit is submitted to establish probable cause that the evidentiary items listed herein were used to commit violations of 18 U.S.C. §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors, among other offenses. The electronic storage devices described herein were seized from Andrew Muzzey and Jacqueline Showalter, after admissions made by Muzzey that chat conversations relevant to enticement of a minor and image(s) of child pornography may be located on such.

3. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A relating to child exploitation and child pornography.

Definitions

4. The following is a non-exhaustive list of definitions that applies to this Affidavit and Attachment A to this Affidavit:

5. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries.

6. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor

engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

7. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

8. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

9. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

10. "Computer" as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

11. "Computer hardware" as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as

any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

12. "Computer software" as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

13. "Computer-related documentation" as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

14. "Computer passwords and data security devices" as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates test keys or hot keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or booby-trap protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

15. "Internet Service Providers" or "ISPs" are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access

the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

16. "Internet Protocol Address" or "IP Address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

17. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Computers and Cell Phones

18. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of

the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. Surveying various file directories and the individual files they contain;

d. Opening files in order to determine their contents;

e. Scanning storage areas;

f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

19. Your Affiant further requests judicial authority to transport/ship these items to any appropriate laboratory setting outside of the Southern District of Illinois, in order to complete a full forensic examination, if necessary.

Details of this Investigation

20. On November 1, 2012, the Madison County Sheriff's Departmetn received information office received from the Illinois Attorney General's Office also known as the Illinois Internet Crimes Against Children Task Force (ICAC) in the form of a "Cybertip" through the National Center for Missing and Exploited Children (NCMEC). The information contained two separate reports of sexual exploitation of a child based on the following information.

21. A social networking mobile application by the name of "AirG" equipped with chatting capability forwarded information to NCMEC regarding the below conversation in reference to Cybertip#1547044:

Drtydad4nwtydwtr: yea
mike3899: yea
Drtydad4nwtydwtr: 9 n up
mike3899: as yung as u want
Drtydad4nwtydwtr: how yng
mike3899: u in to yung yung girl pix

22. The phone number associated to the screename of "Drtydad4nwtydwtr" is 618-233-3483. Based on research conducted, this phone number appears to be owned by Sprint and appears to be tied to the Collinsville area.

23. There was also another conversation in reference to Cybertip#1545423 as documented below as is related to the screename of "Drtydad4nwtydwtr":

Drtydad4nwtydwtr: would love to see her n her little panties
Heather1014: this is tammy
Drtydad4nwtydwtr: wow she is as hot as you. bet your body was killer like hers at that age

24. It was reported that an IP address of 68.28.91.117 was also tied to the above conversation on August 9, 2012, at 16:47:09. "AirG" is reported to be at the location of 1133 Melville St. Suite 710 Vancouver, British Columbia, V6E 4E5 Canada. Sprint conducts business in the State of Illinois.

25. State search warrants directed towards Sprint and AirG were presented to Madison County Circuit Judge Charles Romani and were signed on November 5, 2012.

26. Records were received from Sprint on November 9, 2012. There was no subscriber information associated to the phone. It was a prepaid Boost Mobile Subscriber. Analysis of these records would lead investigators to a person of interest identified as Andrew Scott Muzzey who is white male with a date of birth of [redacted].

27. Andrew Muzzey was ultimately located at a residence located at [redacted]

[redacted] Belleville, Illinois. He was in the company of his fiancé, Jacqueline Showalter. Digital devices were seized at the scene. Specifically, as follows:

1. Black and Silver Apple Ipod, Model: A1367, S/N: C3RHX0NGDT75

2. White and Silver Apple Ipod, Model: A1367, S/N: CCQHWEX1DNQW

3. Black Motorola Boost Mobile Model: WX430 MEID68435460405774382

28. Both subjects were interviewed. According to Jacqueline Showalter, she indicated that Muzzey did set up her white and silver iPod but does not commonly access it. According to Muzzey, he uses the chat client by the name of AirG "dad4nwtydwtr". He indicated that he is the only person that uses this account. He and Jacqueline Showalter have been dating for approximately two years. I asked Muzzey if he has received any images consistent with child pornography. Muzzey said that he may have been sent some but he has deleted them. Muzzey said that he and Jacqueline both use the phone and that at some point he did use the cell phone to access the AirG account. He said that he would role play in a sexual way in a dad and daughter fantasy while chatting. He initially stated that he does not remember the screen names he chatted with but would later provide me with the name of "Heather1014". He said that he was sent one image of a female kid around age fourteen to fifteen with part of her genitalia exposed. Muzzey said that he uses the AirG client with his IPod. According to Muzzey, his IPod is equipped with a text free client application and interfaces with a Magic Jack device for phone usage and that is what he primarily uses.

Conclusion

Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation and I

have set forth the facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A are located within the presently held evidence as described above.

Additionally, your affiant requests that this search warrant affidavit be sealed as this investigation is still on-going. Based on the foregoing information provided, your affiant believes there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A which, among other things, make it a federal crime for any person to knowingly possess and/or receive and distribute child pornography and/or entice a minor, has been violated and that there is evidence, fruits and instrumentalities of these offenses located within the items described herein.

FURTHER AFFIANT SAYETH NAUGHT.

_____
David B. Vucich
Special Federal Officer
FBI Metro-East Cyber Crime and
Analysis Task Force

Ali Summers
Assistant United States Attorney

State of Illinois)
) SS.
County of St. Clair)

Sworn to before me and subscribed in my presence on this _____ day of _____, 2012, at East St. Louis, Illinois.

_____
DONALD G. WILKERSON
United States Magistrate Judge